REMARKS

In the Official Action mailed 21 March 2007, the Examiner reviewed claims 1-21. The Examiner has rejected claims 1-21 under 35 U.S.C. §112, second paragraph; has rejected claims 1-4, 6, 8-11, 13, 15-18 and 20 under 35 U.S.C. §102(b); and has rejected claims 5, 7, 12, 14, 19 and 21 under 35 U.S.C. §103(a).

Applicant has amended claims 1-4, 6-11, 13-18 and 20-21, added claims 22-30, and canceled claim 5, 12 and 19. Claims 1-4, 6-11 and 13-30 remain pending.

The rejections set forth in the Office Action are traversed below, and reconsideration is requested.

Amendments to the Specification

Applicants have amended the specification herein to add the serial numbers of the related applications in the "Related Applications" section of the application herein.

Rejection of Claims 1-21 under 35 U.S.C. §112, second paragraph

The Examiner has rejected claims 1-21 under 35 U.S.C. §112, second paragraph as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicants regard as the invention. Applicant has amended the claims to address the Examiner's concerns.

The claims include a method for producing ephemeral, symmetric encryption keys at a first station for mutual authentication and secure distribution of a random session-specific symmetric encryption key in a communication session with a second station, or logic to distribute symmetric encryption keys (referred to as the final secret key FSK in the present specification) for use in a communication session by the second station, along with a mutual authentication process, using shared secrets and a plurality of exchanges for use in subsequent messages of a communication session between the first and second stations. The procedure recited uses a session key (session random key SRK in the present specification), selected from an set of session keys (array of session random keys ASK in the present specification) stored in a buffer, for a first one of the exchanges in each session initiated within a session key initiation interval, and uses intermediate data keys (data random key DRK in the present specification), a unique set of which (array of data random keys ADEK in the present specification) is associated

with each session key, for following exchanges in the plurality of exchanges, until a final exchange. The intermediate data key used in the final exchange, encrypted using a shared secret credential as stated in the new dependent claim 22 for example, for each communication session becomes the final, symmetric encryption key (FSK) for use by the second station in the communication session.

The claims have been amended to clarify this structure, referring to the symmetric encryption key for use in the communication session, the session key and the intermediate data key where appropriate. The terms "random" and "ephemeral" have been removed in most of the cases as a modifier of "key" for clarity. It is understood that such keys are random or pseudo-random, and short lived in representative embodiments.

Accordingly, reconsideration of the rejection of claims 1-21 as amended is respectfully requested.

Rejection of Claims 1-4, 6, 8-11, 13, 15-18 and 20 under 35 U.S.C. §102(b)

The Examiner has rejected claims 1-4, 6, 8-11, 13, 15-18 and 20 under 35 U.S.C. §102(b) as being anticipated by Perlman (US 6,363,480). Applicant requests reconsideration in light of the amendments.

In particular, the Examiner has interpreted the claims such that the "encryption key" and the "session key" are the same. To the extent the *prima facie* case for anticipation is based on this interpretation, it is incomplete in view of the clarifying amendments. In fact, as explained above, the session key is not used as the symmetric encryption key that is being distributed for use in the communication session. Rather, one of the intermediate data keys is assigned as the final, symmetric encryption key for the communication session.

Perlman is focused on providing an encryption key to a user which the user can apply to encrypting data, but which expires to ensure that the data cannot be decrypted after expiration of the encryption key. The method of providing the encryption key to the user relies on the public key infrastructure, which is an asymmetric key process. Perlman mentions the possibility of using symmetric keys. However, it does not describe a technique for delivering symmetric keys, other than to state that such a key must be "conveyed in a secure manner, for example through a conventional encrypted tunnel mechanism." Column 6, lines 17-20.

The present invention is directed to the problem of distributing ephemeral symmetric keys in the context of a high volume communication system, and producing such keys in a secure and efficient manner. Perlman avoids addressing this problem in detail by referring only to the need to use a "conventional encrypted tunnel mechanism" to deliver a symmetric key. In fact, the present invention and Perlman are addressed to different problems. In the present invention, authentication and symmetric key exchange are concurrent processes in one communication protocol between the first and the second station (or party).

In Perlman, authentication is not considered for the ephemeral public key exchange, because any second station should be able to obtain it from the first station. Hence, the ephemeral public key is not actually a secret. However, if the second station requests an ephemeral symmetric key from the first station, a secure channel to transfer the key is needed according to Perlman (col. 6, lines 17-20) because this key, unlike the ephemeral public key in the previous case, should be a shared secret between these two stations. Otherwise, the message origination and/or the message encryption security can be jeopardized.

Some authentication is essential for the case in Perlman involving symmetric keys. Without authentication, a conventional secure encrypted tunnel cannot be established. However, Perlman does not consider, introduce, propose, or review any conventional or non-conventional authentication process, factor, mechanism, or approach. It is beyond the scope of the Perlman patent.

Moreover, conventional encrypted tunnel security is based on a pre-set static symmetric encryption key stored at both ends of the tunnel, which if compromised make the tunnel vulnerable to intruders. The present invention provides a new method of distributing a random session-specific, symmetric encryption key between first and second stations that provides a great deal more security than a pre-set static key. Hence, it can be said that Perlman does not introduce teaching relevant to the present claims, for a secure delivery of an ephemeral symmetric encryption key over non-secure communication media or infrastructure.

The Office Action refers to Figure 3 of Perlman and its description in columns 5 and 6. As can be seen by a basic review of the Figure, the Perlman process simply involves providing a set of ephemeral keys having key lifetimes at a server, selection by a second party of one of the ephemeral keys, encryption of a message using the selected key and sending the encrypted message to the first party, decryption of the message by the first party using the selected key, and

destruction of the selected key after an expiration time. At column 6, lines 17-20, Perlman contemplates that the second party may select an ephemeral symmetric key, as an alternative to an asymmetric key pair. In this case, Perlman states, "To provide efficient processing, and because symmetric key encryption may be significantly more efficient than public key encryption, the second party may encrypt the message body using a symmetric key (pre-set at the message key portion (col. 5, lines 25-35; Fig. 2, 32)), then encrypt that symmetric key using the ephemeral encryption key, and include the encrypted symmetric key as part of the message, for example in the message header." Thus, Perlman contemplates a process in which a first symmetric key is delivered using a "secure tunneling mechanism" to be used as the "ephemeral encryption key", and a symmetric key at the message key portion is provided by the second party to the first, encrypted by the symmetric key received from the first station. The symmetric key at the message key portion is provided by the second party or user, and not by the server. Also, it is not shared in advance, and therefore does not serve to identify the second party or any other authentication purposes.

Furthermore, Perlman does not describe a technique for producing symmetric keys. In contrast, the claims of the present application describe a procedure for producing a secret symmetric key (FSK) using a plurality of exchanges based on session keys (SRK) having session key lifetimes, and intermediate data keys (DRK) assigned to each session key.

It can be understood therefore that claim 1 distinguishes over Perlman for a number of reasons. First, Perlman does not execute a plurality of exchanges to provide a symmetric encryption key. Rather, the user in Perlman selects an encryption key based on a time limit, and the selected key is delivered to the user either relying on the public key infrastructure for an asymmetric key, or relying on any "secure tunneling mechanism" which is not described for the use of symmetric keys.

The Office Action reads the claim element "session key" on the ephemeral encryption key of Perlman. Thus, the lifetime of Perlman's ephemeral encryption key is relied upon as corresponding to Applicant's "session key initiation interval" of claim 1. However, this is mistaken, because the session key in claim 1 is not used as the final, symmetric encryption key (FSK) for the session. Rather, it is used in a first exchange, provided that the request for establishing a communication session occurs within the corresponding session key initiation interval.

Claim 1 requires that the session key be used for encryption of a "shared parameter," by the second station, which is returned to the first station. This shared parameter is used to verify delivery of the session key and to identify the second station, or the user of the second station, as clarified in the claim as amended. Perlman does not contemplate a similar exchange.

Although Perlman mentions the possibility of using the ephemeral encryption key for the purposes of encrypting a symmetric key for use in a single message, that symmetric key at the message key portion is not a shared parameter capable of use for the purposes of identifying the second station for authentication purposes. Rather, this symmetric key is provided by the second station to the first station, without having been shared in a manner that can be used for authentication purposes.

Claim 1 requires "associating, in the first station, a set of intermediate data keys, different from said session key, with said request for use in said plurality of exchanges." The Office Action sites column 5, lines 55 to column 6, line 20 of Perlman as corresponding to this limitation. The position in the Office Action can only be rationalized by reading the term "session key" of claim 1 as the same as the "intermediate data key". This position is not supportable, particularly in the claims as amended. Perlman describes only the storage of a number of asymmetric key pairs, or in a vaguely described alternative the storage of symmetric keys, in the first station, from which the user selects a single key or key pair based on its time limit. The claimed process of assigning a session key based on the time of the request for initiation of a communication session, and assigning intermediate data keys to each communication session, is not similar to that described in Perlman.

Claim 1 requires sending an encrypted version of one of the intermediate data keys from the first station to the second station to be accepted as the final symmetric encryption key. Because Perlman does not describe the concept of intermediate data keys produced in the first station, it cannot and does not suggest a similar step.

Claims 2-4 and 6 depend from claim 1, and are patentable for at least the same reasons, and because of the unique combinations recited.

Independent claim 8 and claims 9-11 and 13 which depend therefrom, are similar in scope to claims 1, 2-4 and 6, and are patentable for the reasons discussed above. Likewise, independent claim 15 and claims 16-18 and 20 which depend therefrom, are similar in scope to claims 1, 2-4 and 6, and are patentable for the reasons discussed above.

Accordingly, reconsideration of the rejection of claims 1-4, 6, 8-11, 13, 15-18 and 20 as amended is respectfully requested.

Rejection of Claims 5, 7, 12, 14, 19 and 21 under 35 U.S.C. §103(a)

The Examiner has rejected claims 5, 7, 12, 14, 19 and 21 under 35 U.S.C. §103(a) as being unpatentable over Perlman. Claims 5, 12 and 19 are canceled. Claims 7, 14, and 21, depend from claims discussed above, and are patentable for at least the same reasons as their base claims.

Accordingly, reconsideration of the rejection of claims 7, 14 and 21 as amended is respectfully requested.

New Claims 22-30

New claims 22-30 recite embodiment of exchanges in the plurality of exchanges in which the final, symmetric key distributed for use in the communication session is sent as an encrypted version of one of the intermediate data keys. The new claims are supported by the original specification at paragraphs [0038], [0047], [0073-0075], and Fig. 3 and Figs. 8A-8B.

CONCLUSION

It is respectfully submitted that this application is now in condition for allowance, and such action is requested.

The Commissioner is hereby authorized to charge any fee determined to be due in connection with this communication, or credit any overpayment, to our Deposit Account No. 50-0869 (AIDT 1005-1).

Respectfully submitted,

/mark haynes/

Dated: 8 June 2007

Mark A. Haynes, Reg. No. 30,846

HAYNES BEFFEL & WOLFELD LLP
P.O. Box 366
Half Moon Bay, CA 94019
(650) 712-0340 phone
(650) 712-0263 fax